REMARKS

Status of the Claims

- Claims 53 and 55-84 are pending in the Application after entry of this amendment.
- Claims 53, 55-58, 62-68, 70, 71, 74, 75, 78, 79, 83, and 84 are rejected by Examiner.
- Claims 59-61, 69, 72, 73,, 76, 77, and 80-82 are objected to.
- Claims 53, 55-69, and 74-84 are amended by Applicant.
- Claim 54 is cancelled.

Allowable Subject Matter

Claims 59-61, 69, 72, 73,, 76, 77, and 80-82 stand objected to as being dependent upon a rejected base claim, but are identified as being allowable subject matter. Applicant amends the respective base claims to overcome the objection.

Claim Rejections Pursuant to 35 U.S.C. §102

Claims 53, 55-58, 62-68, 70, 71, 74, 75, 78, 79, 83, and 84 stand rejected under 35 U.S.C. § 102 as being anticipated by U.S. Patent No. 7,054,461 to Zeller et al. (Zeller). Applicant respectfully traverses the rejection via amendment.

Citations to Applicants' Specification in the following are to the PCT publication of the International Stage of this application, WO05067586. Applicants will first demonstrate support for the amended claims, then set forth what Applicants are claiming using claim 55 as an example, and will then show that Zeller does not disclose what is being claimed.

Support for the claims as amended

Applicants' claim 55 as amended reads as follows:

55. (currently amended). A method of creating a digital authentication pattern that permits non-watermark-based determination of a copying relationship of a digital representation of an object with which the digital authentication pattern is associated, the digital authentication pattern containing a message, the digital authentication pattern belonging to a digital representation of an object with which the digital authentication pattern is associated, and the digital authentication pattern including a plurality of pattern elements that have pattern element values and the method comprising:

selecting a set of the pattern elements to represent message elements of the message; and

for a pattern element belonging to the selected set of pattern elements, setting the pattern element's pattern element value to represent the message element such that setting the pattern element's value to represent the message element leaves the digital authentication pattern's usefulness in determining the copying relationship substantially unchanged.

Support for the claims as amended

Disclosure for what is claimed in this application may principally be found in the section *Technique for inserting information into a VAP,* at pages 41-45 of the PCT publication of this application, WO05067586. The claim language is supported by the disclosure as follows: the term "digital authentication pattern" is a generic term that includes the VAP and many analogous structures; see page 50 of WO05067586. The pixel blocks described at page 41, lines 28-34 are embodiments of the digital authentication pattern's "pattern elements". A "message element" is a pattern element whose pattern element value represents a "message element value". The claim terms appear in the claims as originally filed in the PCT application.

As set forth at page 41, lines 15-25, an important feature of the techniques disclosed at pages 41-45 is that the addition of the message to the digital authentication pattern "leaves the digital authentication pattern's usefulness in determining the copy relationship substantially unimpaired". The term "copying relationship" appears in the application's Abstract and at page 3, line 5. The term is used to indicate the fact that the "digital authentication pattern" can be used to determine not only whether the digital representation associated with the digital authentication pattern is a copy, but also other information such as the generation of the copy See in this regard the discussion at page 51, line 25-page 52, line 2.

Applicants' disclosure

As set forth in the *Cross references to related applications* on page 1 of WO2005/067586, Applicants' application is directed to improvements in the visual authentication pattern (VAP). The VAP is the invention described in PCT/US03/15186 and published as WO2003/098540. WO2005/067586 contains substantial portions of the Specification of WO2003/098540. The new

material in WO2005/067586 begins with the section *Detecting the position of a VAP* at page 28. The claims of the present invention are directed to techniques for inserting information into a digital authentication pattern. As described beginning at page 41, the techniques are directed to inserting information into a VAP. The VAP is a species of the "digital authentication pattern" of Applicants' claims; how the techniques which are embodied in the VAP for authenticating copies of printed documents may be generalized to apply to other media is explained at pages 49-50.

The *Cross references to related applications* of WO2005/067586 makes it clear that the VAP described in WO2003/098540 is prior art with regard to the present patent application. In the present application, the *Description of related art* describes a VAP as follows (page 1, line 27-page 2 line 2)

> Visible Authentication Patterns (VAPs) can be used to determine whether a printed document has been altered or whether the document is an original or a copy. A VAP is a noisy pattern in a portion of a digital document. It is used to determine the authenticity of a document by comparing a portion of a digital recording made from the analog form with an original digital representation of the portion of the analog form to determine a degree of dissimilarity (or similarity) between the recorded portion and the original digital representation of the portion and using the degree of dissimilarity (or similarity) to determine whether the analog form is an original analog form.

From the foregoing, it is clear that the VAP is not a digital watermark. It should further be noted that there is no indication in the above or anywhere else in either WO2003/098540 or WO2005/067586 that using a VAP to determine whether an analog form is an original analog form in any way involves determining the condition of a watermark.

The portion of WO2003/098540 which is included in WO2005/067586 further includes a description at page 25 of how a watermark may be included in a VAP; as pointed out there (lines 11-13),

> When a digital watermark is embedded into to a VAP, the VAP will be slightly modified. As a result, when the same VAP is used for authenticity verification, its reliability for that purpose may be reduced.

The claims of the present patent application are thus directed neither to VAPs nor to using watermarks in VAPs, but are rather directed to digital authentication patterns which can carry messages without reducing the digital authentication pattern's reliability when used to verify the authenticity of a copy and thereby overcome the problem set forth in WO2003/098540. It should be particularly noted at this point that as is apparent from the discussion of the problem at page 25 and the discussion of the solution at pages 41-45, the copying relationship of the document carrying the VAP *is not* determined from the condition of the message which is inserted into the VAP.

What claims 55-84 in the present patent application address is techniques for adding a message to the digital authentication pattern while "leav[ing] the digital authentication pattern's usefulness in determining the copy relationship substantially unimpaired" This distinction from WO2003/098540 is set forth in the italicized portion of claim 55:

> 55. (currently amended). A method of creating a digital authentication pattern that permits non-watermark-based determination of a copying relationship of a digital representation of an object with which the digital authentication pattern is associated, the digital authentication pattern containing a message, the digital authentication pattern belonging to a digital representation of an object with which the digital authentication pattern is associated, and the digital authentication pattern including a plurality of pattern elements that have pattern element values and the method comprising:
>
> selecting a set of the pattern elements to represent message elements of the message; and
>
> for a pattern element belonging to the selected set of pattern elements, *setting the pattern element's pattern element value to represent the message element such that setting the pattern element's value to represent the message element leaves*

> *the digital authentication pattern's usefulness in determining the copying relationship substantially unchanged.*

How the setting is done in a preferred embodiment is set forth in claim 56, which states that "the pattern element value is set such that the entropy of the digital authentication pattern is substantially unchanged". The meaning of "entropy" in this context is set forth at page 29, lines 8-18:

> As used here, entropy is the probability that a pixel in a block of a grayscale image will have a one of a large number of different values. In a block that contains print (printed text or graphics), for example, the pixels will typically be concentrated around two values, i.e. near white if they represent paper and near black if they represent print, and thus the probability that a pixel will have one of a large number of values is low and so is the entropy. Because the VAP in a digital representation is noisy, there is a high probability that a pixel in the VAP will have one of a large number of values, and the VAP's entropy is high.

What Zeller discloses

Citations to Zeller in the following are to paragraphs in the U.S. patent application publication of his disclosure, US 2003/0156733 A1, published Aug. 21, 2003. What Zeller discloses is well set forth by his title, *Authenticating printed objects using digital watermarks associated with multidimensional quality metrics*, and his *Abstract:*

> The disclosure describes an authentication system and related methods for authenticating printed objects. The system uses an information-based metric along with one or more print quality metrics to provide accurate detection or classification of a counterfeit printed object. The print quality metric evaluates attributes of a subject image associated with the original printer, ink or paper to detect degradation of those operations due to copying operations like an image scanning and halftone printing subsequent to the original printing of the object. The information-based metric measures message symbol errors in an optically readable code, such as a digital watermark.

As is clear from the foregoing, Zeller is directed to techniques for solving the same problem that is solved by Applicants' techniques, namely "detection of

copies of the digital representation", but Zeller's techniques take a completely different approach:

- Applicants' techniques use digital authentication patterns, which are not watermarks, to detect copies and also provide ways of including information in the digital authentication patterns. The included information has two properties: the information as included does not affect the usefulness of the digital authentication patterns to detect copies and the condition of the included information is not relevant to copy detection.
- Zeller's techniques use watermarks to detect copies and as would be expected, copy detection is based on the condition of the watermarks. There is simply no equivalent to Applicants' digital authentication patterns in Zeller.

That Zeller and Applicants take the different approaches set forth above is immediately apparent when Applicants' FIG. 4, included in both WO2003/098540 and WO2005/067586, is compared with Zeller's FIG. 1. Applicants' FIG. 4, discussed beginning at page 9, line 26, shows Applicants' prior art techniques for copy detection; Zeller's FIG. 1, discussed beginning at [0033], shows Zeller's techniques. The chief difference between them is that FIG. 1 uses watermarks for copy detection and FIG. 4 uses digital authentication patterns. In FIG. 1, the first step, at 102, is to "embed digital watermark" in the original. When an unauthorized copy is to be detected, it is done using the Zeller "watermark decoder" at 114. As set forth at [033], "Fig. 1 is a diagram illustrating creation and authentication of printed articles using print quality metrics *in combination with an information-based metric derived from digital watermarks embedded in an image*." (emphasis added) The technique of FIG. 1 thus has at its core the use of an embedded watermark to detect copying.

FIG. 4, by contrast employs VAPs rather than watermarks. The VAP from the digital representation of the original document (ovap 45) is compared with a VAP from a digital representation of the copy being checked (roavap 415, novap 425, noavap 431, moavap 435). The degree of difference indicates whether the analog form is an original analog form or a non-original analog form. No watermarks are involved in FIG. 4, just as no VAPs are involved in FIG. 1.

As already indicated, FIG. 4 is prior art with regard to the present application. The *entire point* of the inventions of claims 55-84 is to provide a technique for adding a message to a VAP which *has no effect* on the prior-art technique shown in FIG. 4. Claim 55 is distinguished from the technique shown in FIG. 4 in that the VAP contains a message. The values of the pattern elements making up the message, however, are set such that "*the digital authentication pattern's ability to detect copying remains substantially unchanged*", which means that the technique shown in FIG 4 can still be applied to the VAP.

As regards Zeller, claim 55 is distinguished from Zeller first, by the use of a digital authentication pattern, second by the fact that "the digital authentication pattern permit[s] non-watermark-based detection of copies of the digital representation", and third by the fact that "the pattern element's values are set such that the digital authentication pattern's ability to detect copying remain substantially unchanged" Because Zeller does not disclose the foregoing limitations, Zeller does not anticipate claim 55. As Examiner will immediately see, the same argument applies with regard to independent claims 66 and 75 as well. Claim 53 as amended similarly recites that the "copy detection signal" of the claim's "sensitivity to transformations produced by digital-to-analog and analog-to-digital conversions is not based on a watermark contained in the copy detection signal".

Independent patentability of the dependent claims over Zeller

Claims 56 and 67

These claims add the feature that "the entropy of the digital authentication pattern is substantially unchanged" as a result of setting the pattern element value. The first issue here is that there is no digital authentication pattern in Zeller, and consequently, nothing to add the limitation of these claims to. The second issue is that the only mention of "entropy" in Zeller is the following, at [0109]:

> For forensic purpose, multiple scans permit generation of a more accurate image because several images of a watermark, together potentially contain more information than a single image. The resolution enhancement procedure, which is a process of intelligent image fusion, permits recovery of image information by minimizing the entropy of a set of piled-up images with respect to their respective registration. Improved information about the image formation process (i.e. if the image has been generated from a scanned image or directly printed from a bit map) can be gained from this procedure.

Clearly, a "resolution enhancement procedure which … minimize[es] the entropy of a set of piled up images with respect to their respective registration" has nothing whatever to do with setting pattern element values in the sets that carry message elements such that "the entropy of the digital authentication pattern is substantially unchanged", as set forth in claims 56 and 57; consequently, the added limitation of these claims are lacking in Zeller.

Claims 57-63 and 68-69

The features added in these claims all have to do with the manner in which the message is added to the digital authentication pattern "such that the digital authentication pattern's ability to detect copying remains substantially unchanged". Zeller does not add a message to a digital authentication pattern. Beginning at [0123], Zeller does disclose techniques for embedding and detecting digital watermarks. As set forth at [0126], watermark generation in

Zeller is governed by "visibility and detectability constraints" for the watermark; as noted above, in Applicants' claims, the governing constraint is that "the digital authentication pattern's ability to detect copying remains substantially unchanged"; consequently, Zeller does not disclose the added features of claims 57-63 and 68-69 and these claims are novel in their own rights over Zeller.

Claims 76-83

The features added in these claims have to do with techniques for constructing "an equivalent digital authentication pattern to the digital authentication pattern that contains the message" and then comparing the equivalent digital authentication pattern with the digital authentication pattern that contains the message to determine the copying relationship. There is of course no comparison of digital authentication patterns in Zeller, and consequently, Zeller does not disclose the added limitations of claims 76-83.

Conclusion

Applicants have amended their claims to better distinguish them from Zeller, have demonstrated that their claims as amended are fully supported by the Specification as originally filed, and have demonstrated that Zeller does not disclose all of the features of the claims as amended and consequently does not anticipate the amended claims. Applicant respectfully submits that the pending claims patentably define over the cited art and respectfully requests reconsideration and withdrawal of all rejections of the pending claims. Applicant suggests that since the pending claims patentably define over the cited art, that reconsideration be provided for a Notice of Allowance of all pending claims.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 07-0832 therefore.

Respectfully submitted,
Justin Picard
Jian Zhao

Date: May 21, 2010

/Jerome G. Schaefer/
Jerome G. Schaefer
Attorney for Applicant
Reg. No. 50,800
(609) 734-6451

Thomson Licensing, LLC
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312